ABSTRACT OF THE DISCLOSURE

A system can process a digital representation (DF) of a document with a one-way cryptographic hash function (CHF) to yield a digital fingerprint (DFP) value that is associated with the DF. A document identification number (DID) is created, uniquely associated with the DFP, and with DID and DFP are associated optional credential information (C). A registration certificate DFC that represents an optional electronic signature associated with the document and that includes the DID and DFP is promulgated and archived at a plurality of storage locations. The system can authenticate whether a putative document is the original document by generating a digital fingerprint value for the putative document and comparing it to DFP retrieved from various of the storage locations. Authentication can confirm that the electronic signature is unaltered.